FIG. 1

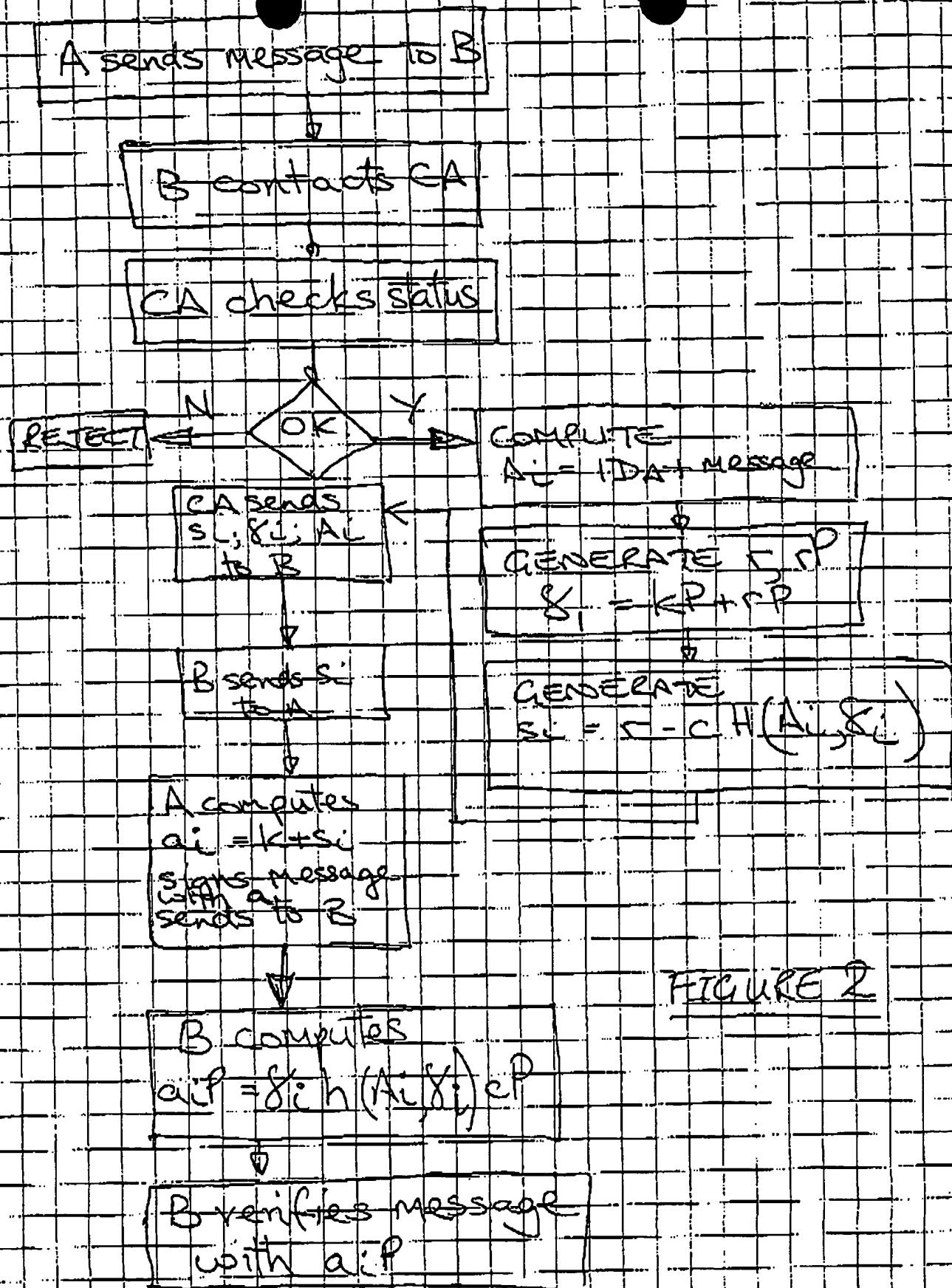


FIGURE 2

A sends IDA and k^P
to CA

A requests certificate
from CA

CA computes s_i, δ_i, A_i
and sends to A

A signs message M
with $a_i = k + s_i$

A sends signed M, δ_i
and A_i to B

B computes a_i^P
using A_i, δ_i

B verifies message
with a_i^P

FIGURE 3

A sends ID_A and KP to CA

A requests certificate from CA

CA uses ID_A and a permission level to determine A_i

CA generates s, s_i base on A_i and send all 3 to A

A signs message, m, with
 $a_i = k + s_i$

A sends signed m, s_i and A_i to B

B computes a_{iP} using A_i, s_i

B verifies message with a_{iP}

B grants A access to an application

FIGURE 4

A generates random integer a

A transmits aP and A_i to the CA

CA generates S_A and S_A and transmits them to A

A generates private key $d = a + S_A$
public key $Q_A = dP$

FIGURE
5

A signs message with d

A sends signed message S_A and A_i to B

B derives Q_A using S_A , A_i and CA's public key Q_c

B verifies A using Q_A

A acquires δ_A, S_A from CA
computes $d = a + S_A$

certification period = i

CA calculates S_{A_i} and Q_i

CA transmits S_{A_i} to A
publishes Q_i and

A signs message with
 $d = a + S_{A_i}$

FIGURE 6

A sends signed message, δ_A ,
and A_i to B

B uses δ_i, A_i, i, Q_i and CA's
public key Q_C to determine
A's public key Q_A

B verifies A using Q_A

certification period = $i+1$